**No. 25-1411**

**IN THE UNITED STATES COURT OF APPEALS**
**FOR THE FOURTH CIRCUIT**

---

AMERICAN FEDERATION OF STATE, COUNTY AND MUNICIPAL EMPLOYEES, AFL-CIO, et al.,

Plaintiffs-Appellees,

v.

SOCIAL SECURITY ADMINISTRATION, et al.,

Defendants-Appellants.

---

On Appeal from the United States District Court
for the District of Maryland

---

# BRIEF FOR APPELLANTS

---

YAAKOV M. ROTH
*Acting Assistant Attorney General*

ERIC D. MCARTHUR
*Deputy Assistant Attorney General*

GERARD SINZDAK
JACK STARCHER
SIMON JEROME
JACOB CHRISTENSEN
*Attorneys, Appellate Staff*
*Civil Division, Room 7525*
*U.S. Department of Justice*
*950 Pennsylvania Avenue NW*
*Washington, DC 20530*
*(202) 514-5048*

# TABLE OF CONTENTS

**Page**

## TABLE OF AUTHORITIES

**Cases:** **Page(s)**

**Statutes:**



**Regulatory Materials:**

**Other Authorities:**

## INTRODUCTION

The district court enjoined particular agency employees—the 11 members of the Social Security Administration DOGE (Department of Government Efficiency) team—from accessing data that plaintiffs' members willingly turned over to the Social Security Administration (SSA) for government use, that other agency employees can unquestionably access consistent with law, and that the SSA DOGE team will (and can) only use for legitimate and lawful purposes. In imposing this sweeping inunction, the district court assumed the power to micro-manage Executive agency operations, including dictating to the Executive Branch which government employees can access which data—even prescribing training, background checks, and onboarding paperwork for data access. (JA1294–1295.)

That injunction is barred by multiple independent barriers to judicial review of plaintiffs' claims. First and foremost, plaintiffs have failed to show an Article III injury-in-fact. Plaintiffs assert their members will be harmed if the personal information they voluntarily shared with SSA is viewed *internally* by *certain* SSA employees, but that theory of injury bears no resemblance to any injury recognized at

common law. At bottom, plaintiffs allege only a bare statutory violation, which the Supreme Court has unequivocally rejected as a sufficient basis for federal court jurisdiction. *See TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021). That injunction also embraces a precedent-defying view of what constitutes reviewable "final agency action" under the Administrative Procedure Act (APA). The Supreme Court and this Court have long held that the APA is not a vehicle for challenging day-to-day operational decisions. Nor do those mundane operational decisions have any of the features courts have deemed necessary for finality—they do not create any rights or obligations, nor do any legal consequences flow from them.

Finally, even if the district court had the authority to adjudicate this case, its injunction rests on a deeply flawed reading of the Privacy Act. The Executive Branch, not district courts, sets government employees' job responsibilities, and nothing in the Privacy Act authorizes district courts to second-guess whether particular government employees really need particular records to perform their responsibilities.

On June 6, 2025, the Supreme Court granted the government's application to stay the district court's preliminary injunction, concluding that a stay was warranted under the stay factors in *Nken v. Holder*, 556 U.S. 418, 434 (2009). *See Social Security Admin. v. Am. Fed'n of State, Cnty., & Mun. Emps.*, No. 24A1063, 605 U.S. __ (2025). As the Supreme Court's ruling foreshadows, the district court's preliminary injunction was an abuse of discretion and should be vacated.

## STATEMENT OF JURISDICTION

Plaintiffs invoked the district court's jurisdiction under 28 U.S.C. § 1331 (JA23), but the government contests the district court's jurisdiction over plaintiffs' claims. The district court granted plaintiffs' motion for a preliminary injunction on April 17, 2025 (JA1293–1298), and the government timely appealed that same day (JA1447). This Court has jurisdiction under 28 U.S.C. § 1292(a)(1).

## STATEMENT OF THE ISSUES

This appeal raises the following issues regarding whether the district court abused its discretion in entering a preliminary injunction:

(1) Whether plaintiffs have Article III standing;

(2) Whether plaintiffs' claims are subject to judicial review under the APA;

(3) Whether the Social Security Administration violated the Privacy Act or the APA;

(4) Whether plaintiffs faced irreparable harm and satisfied the remaining preliminary injunction factors.

## PERTINENT STATUTES AND REGULATIONS

Pertinent statutes and regulations are reproduced in the addendum to this brief.

## STATEMENT OF THE CASE

### A. Executive Order 14,158

On January 20, 2025, the President signed Executive Order 14,158 establishing the Department of Government Efficiency (DOGE) to implement the President's "18-month DOGE agenda" by "modernizing Federal technology and software to maximize governmental efficiency and productivity." Exec. Order No. 14,158, §§ 1, 3(b), 90 Fed. Reg. 8441, 8441 (Jan. 29, 2025). The Executive Order renamed the preexisting United States Digital Service as the United States DOGE Service (USDS), moved it out of the Office of Management and Budget, and established it within the Executive Office of the

President. The Executive Order also established within USDS a temporary organization known as "the U.S. DOGE Service Temporary Organization." *Id.* § 3(a), (b).

The Executive Order requires each "Agency Head"—*i.e.*, the highest-ranking official in each agency—to establish "within their respective Agencies" a "DOGE Team" consisting of at least four "employees" (which may include special government employees). Exec. Order No. 14,158, §§ 2(b), 3(c). The Executive Order further charges the USDS Administrator with "commenc[ing] a Software Modernization Initiative to improve the quality and efficiency of government-wide software, network infrastructure, and information technology (IT) systems." *Id.* § 4(a). And the Executive Order directs the USDS Administrator to collaborate with agency heads to modernize the technology and software infrastructure to "promote inter-operability between agency networks and systems, ensure data integrity, and facilitate responsible data collection and synchronization." *Id.*

To accomplish those objectives, the Executive Order also directs the USDS Administrator and agency heads to work together to ensure that USDS has access to "unclassified agency records, software systems,

and IT systems" to the "extent consistent with law." Exec. Order No. 14,158, § 4(b). And it provides that "USDS shall adhere to rigorous data protection standards." *Id.*

The Executive Order addresses the government's well-documented, urgent need to update and improve its information technology systems to promote efficiency and identify fraud. The Government Accountability Office (GAO) has found that "improper payments and fraud are long-standing and significant problems in the federal government," with "cumulative improper payment estimates by executive branch agencies" totaling about $2.7 trillion since fiscal year 2003. GAO, GAO-24-107660, *Payment Integrity: Significant Improvements Are Needed to Address Improper Payments and Fraud*, at i (Sept. 10, 2024), https://perma.cc/XC6R-DXK8. Most relevant here, the GAO has identified SSA's Supplemental Security Income program as one of six program areas that together "were responsible for approximately $200 billion of the $236 billion fiscal year 2023 improper payments estimate." *Id.* The GAO therefore found it "critical that actions are taken to enhance payment integrity and reduce improper payments in these programs." *Id.* at 10.

### B. SSA's DOGE Team

To carry out the President's Executive Order, the SSA established a DOGE team within SSA consisting of 11 SSA employees (initially there were 10) who are responsible for implementing the President's 18-month DOGE agenda. (JA121, JA388.) Each of these employees was onboarded with SSA in February or March 2025, either as an expert appointed under 5 U.S.C. § 3109 or as a detailee from another government agency or office under the Economy Act, 31 U.S.C. 1535. (JA121–123; *see also* JA517, JA574–627, JA642–649, JA1070–1098.) These highly specialized individuals are employed by SSA on a time-limited basis and, therefore, must be able to act swiftly to ensure they complete their responsibilities at SSA within the duration of their employment.

As part of their onboarding, each member of the DOGE team at SSA received the same level of training that is typically required of other SSA employees who are granted access to SSA systems of record. (JA119 (Declaration of SSA Chief Information Officer Michael Russo), JA123 (Declaration of SSA Deputy Commissioner of Human Resources Florence Felix-Lawson), JA402.) The training covered applicable

privacy and ethics laws governing agency employees and data, and each DOGE team member signed certificates of completion for the training and agreed to abide by SSA's information security and privacy policies. (JA119, JA123, JA402, JA1099–1146, JA1152–1156.)

In accordance with its practice, SSA also initiated background investigations of the DOGE team members. (*See* JA124.) When SSA onboards a new employee, it conducts a prescreening check and then releases the background check to the Federal Bureau of Investigation or the Defense Counterintelligence and Security Agency for a full investigation, which normally takes months or up to a year to complete. (JA402–403.) SSA's practice is that during this time, while waiting for the full investigation to be completed, the new employee may work and may have access to SSA's systems, including personally identifiable information. (JA403 (Declaration of SSA Deputy Commissioner of Human Resources Florence Felix-Lawson).) The record indicates that full background checks for the DOGE team members are pending. (*See* JA124, JA401–404.)

On various dates in February and March 2025, SSA's Acting Commissioner approved a series of requests authorizing specific

members of the DOGE team to access certain SSA systems of record, including records containing personally identifiable information of individuals, for the various purposes stated in the requests. (JA542–573, JA113–118; *see also* JA1422–1427.) The requests explained the need for such access. (JA542–573.) SSA declarations submitted in the district court also describe the projects assigned to DOGE team members at SSA and why access to personally identifiable information, without anonymization, is necessary to accomplish them. (JA113–119, JA396–400, JA453–456, JA458–460; *see also* JA518–526.) The level of access to SSA systems given to DOGE team members has also been given to a number of other SSA employees. (JA119.)

### C. Prior Proceedings

#### 1. The complaint

Plaintiffs, "two national labor and membership associations and one grassroots advocacy organization" (JA1303), filed this lawsuit on February 1, 2025, and then filed an amended complaint on March 7, 2025 (JA20–50.) As relevant here, the amended complaint alleges violations of the APA, 5 U.S.C. § 706(2), and the Privacy Act, 5 U.S.C. § 552a. (JA42–45.)

### 2. The temporary restraining order

On March 20, 2025, the district court granted plaintiffs a temporary restraining order (TRO) enjoining the SSA and related defendants from permitting DOGE team members to access certain SSA records. (JA236–241.) Specifically, the TRO prohibited the SSA from granting access to any SSA system of records to "DOGE," USDS, "members of the DOGE Team established at" the SSA, certain named individuals, and "any DOGE Affiliate," defined to include any SSA employee working "directly or indirectly" with the DOGE team, unless a host of judicially imposed conditions were met. (JA237.)

Defendants appealed and sought a stay of the district court's TRO pending appeal. On April 1, 2025, this Court dismissed the appeal for lack of jurisdiction. (JA461–462.)

### 3. *AFT v. Bessent*

Meanwhile, another court in the same District entered a preliminary injunction in a case raising nearly identical legal questions as this one. *American Fed'n of Teachers (AFT) v. Bessent*, Civ. No. 25-430, 2025 WL 895326 (D. Md. Mar. 24, 2025). That preliminary injunction enjoined the Department of Education, the Department of

the Treasury, and the Office of Personnel Management from "disclosing the personally identifiable information of the plaintiffs and the members of the plaintiff organizations to any DOGE affiliates, defined as individuals whose principal role is to implement the DOGE agenda as described in Executive Order 14,158 and who were granted access to agency systems of records for the principal purpose of implementing that agenda." *Id.* at *32–33.

The government appealed the preliminary injunction in *Bessent*, and this Court granted the government's motion to stay the injunction pending appeal. *AFT v. Bessent*, No. 25-1282, 2025 WL 1023638 (4th Cir. Apr. 7, 2025). Judge Agee and Judge Richardson each wrote opinions concurring in that decision, in which the other joined. Judge Agee concluded that all traditional stay factors favored the government and that, in particular, the government had made a "strong showing that it will succeed on the merits as to standing." *Id.* at *1; *see id.* at *3. Judge Agee emphasized that the district court's determination that the plaintiffs could demonstrate a concrete Article III injury based on which government employees could access their data contravened *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021), and circuit precedent. *Bessent*,

2025 WL 1023638, at *1. Judge Richardson agreed that the plaintiffs "seemingly lack[ed] standing," *id.* at *4, and he found that the government was likely to prevail on additional issues, including whether the data access decisions constituted final agency action, *id.* at *5; whether the Privacy Act's comprehensive remedial scheme precluded an APA cause of action, *id.* at *6; whether the agencies violated the Privacy Act, *id.*; and whether the plaintiffs faced irreparable harm, *id.* at *6–7.

Judge King dissented from the panel's decision to grant a stay. *Bessent*, 2025 WL 1023638, at *1, *7.[1]

**4. The preliminary injunction**

Ten days after this Court stayed the *Bessent* injunction, the district court here issued a materially similar injunction, based on nearly identical reasoning and analysis as that deployed by the district court in *Bessent*. (JA1293–1298, JA1299–1446.) Specifically, the district court here found that the plaintiff organizations had standing on behalf of their members by analogy to the tort of intrusion upon

[1] Judge King sought initial en banc consideration of the government's motion for a stay, which this Court denied by a vote of 8-7. *Bessent*, 2025 WL 1023638, at *1, *7.

seclusion (JA1347–1383); that agency decisions to grant access to particular employees were final agency action (JA1392–1403); that plaintiffs were likely to succeed on the merits of their Privacy Act and APA claims (JA1410–1436); that plaintiffs would suffer irreparable harm absent an injunction (JA1436–1440); and that the balance of the equities and the public interest favored an injunction (JA1441–1444).

The district court said that "this case differs markedly" from *Bessent* for three principal reasons, without explaining why those reasons mattered to the legal analysis. (JA1305.) First, the court found that "virtually from its inception, SSA has been guided by an abiding commitment to the privacy and confidentiality of the personal information entrusted to it by the American people." (JA1305.) Second, the court thought it relevant that "this case involves access to personal information of children" who receive benefits through SSA. (JA1306.) Third, "this case involves SSA's access, *inter alia*, to extensive medical and mental health records of SSA beneficiaries" (JA1306)—which the court viewed as not "central" in *Bessent* (JA1376).

The district court enjoined SSA from granting access to any SSA system of records containing personally identifiable information to

DOGE, USDS, the U.S. DOGE Service Temporary Organization, "members of the DOGE Team" at SSA, Elon Musk, Amy Gleason, and "any DOGE Affiliate(s)." (JA1293–1294.) The court ordered the DOGE defendants, SSA DOGE team members, and DOGE affiliates to "disgorge and delete all non-anonym[ous]" personally identifiable information they had obtained from an SSA system of record since January 20, 2025, and enjoined them from installing software on SSA devices or accessing or disclosing SSA computer or software code.[2] (JA1294.) Like the TRO, the preliminary injunction allows SSA to provide DOGE team members with access to certain data and records only if a host of judicially imposed conditions are met.[3] (JA1294–1295.)

Defendants timely appealed and sought a stay of the district court's injunction from both that court and this Court. (JA1447–1449); Motion for Stay, No. 25-1411 (4th Cir. Apr. 18, 2025), Dkt. 6. The

[2] The "DOGE defendants" (U.S. DOGE Service, U.S. DOGE Service Temporary Organization, Elon Musk, and Amy Gleason) have never had access to SSA systems of record. (JA388.)

[3] While the TRO was in place, defendants notified the district court that, as to four DOGE team members, SSA satisfied the access criteria imposed by the TRO. (JA1308.) The court construed that filing as a "request to provide access to four DOGE Team members" and denied it as moot as part of the preliminary injunction order. (JA1296.)

district court denied the motion to stay. On April 30, 2025, this Court granted initial hearing en banc and denied the motion to stay by a vote of 9-6. Order Denying Stay, No. 25-1411 (4th Cir.), Dkt. 20.

Judge King filed a concurring opinion, in which six other judges joined. On his view, "DOGE's work could be accomplished" without the access to data that the agency has deemed appropriate and necessary. Order Denying Stay 7, Dkt. 20. Although Judge King "continue[d] to believe that the stay motion in *Bessent* was worthy of initial en banc consideration and that the stay should not have been granted," he distinguished the cases on the ground that SSA's records include many millions of people, whereas "the *Bessent* injunctive relief, by contrast, was limited to the two million or so plaintiffs." *Id.* at 11–12. Judge Wynn and Judge Heytens each issued concurring opinions focused on the decision to consider the stay motion en banc. *Id.* at 13–15.

Judge Richardson issued a dissenting opinion in which five other judges joined. He explained that although "this case comes in different clothing, it is the legal twin of" *Bessent*, so that to succeed on their preliminary injunction, plaintiffs would have to "beat the same long odds as their counterparts" in *Bessent*. Order Denying Stay 16–17, Dkt.

20. As in that case, "standing is a daunting hurdle all on its own." *Id.* at 17. Specifically, plaintiffs' analogy to intrusion upon seclusion failed, as "no plaintiff has alleged that they have been the subject of any targeted snooping" or even "that a DOGE-affiliated SSA employee has seen their specific personal information." *Id.* at 20. He further explained that while "SSA's databases are larger" than the databases at issue in *Bessent*, they contain the same types of sensitive information, and "the jurisdiction and statutory interpretation questions before [the Court] presumably come out the same whether [the databases] contain one million rows or one hundred million rows." *Id.* at 18. Judge Richardson therefore would have "treat[ed] like things alike" and stayed the injunction in this case. *Id.* at 20.

On June 6, 2025, the Supreme Court granted the government's application to stay the district court's preliminary injunction pending the disposition of this appeal and the disposition of any petition for a writ of certiorari. *Social Security Admin. v. Am. Fed'n of State, Cnty., & Mun. Emps.*, No. 24A1063, 605 U.S. __ (2025). The Court held that a stay was warranted after applying the stay factors in *Nken v. Holder*, 556 U.S. 418, 434 (2009)—"(1) whether the stay applicant has made a

strong showing that he is likely to succeed on the merits; (2) whether the applicant will be irreparably injured absent a stay; (3) whether issuance of the stay will substantially injure the other parties interested in the proceeding; and (4) where the public interest lies." The Court thus concluded that "SSA may proceed to afford members of the SSA DOGE Team access to the agency records in question in order for those members to do their work." *Social Security Admin*, No. 24A1063, 605 U.S. __, slip op. at 2.

## SUMMARY OF ARGUMENT

The district court's preliminary injunction was an abuse of discretion and should be vacated.

I. To obtain a preliminary injunction, plaintiffs had the burden of establishing, among other things, that they have Article III standing, that the agency decisions they challenge constitute final agency action that is reviewable under the APA, and that granting DOGE team members access to information systems those employees are tasked to improve violates the Privacy Act or the APA. Plaintiffs are not likely to prevail on *any* of these issues, let alone *all* of them.

A. The district court wrongly concluded that plaintiffs suffered an Article III injury-in-fact that allows them to assert their claims in federal court. To demonstrate standing, plaintiffs had to show that the injury they allege bears a close relationship to a harm recognized at common law. *See TransUnion LLC v. Ramirez*, 594 U.S. 413, 417 (2021). Plaintiffs have not done that; they allege only an intangible privacy harm arising from the SSA allowing certain SSA employees to access SSA data systems containing personal information that plaintiffs' members voluntarily submitted to the SSA with full knowledge that the information could be routinely accessed by agency employees to perform their responsibilities. That amorphous privacy harm is not analogous to any common law cause of action—certainly not the tort of intrusion upon seclusion, which requires an encroachment into a person's private space that would be highly offensive to a reasonable person.

B. Plaintiffs also fail to identify a "final agency action" reviewable under the APA. 5 U.S.C. § 704. The government actions plaintiffs challenge—a loosely defined series of personnel decisions related to granting individual employees access to agency systems—are

the kind of day-to-day intra-agency operational decisions that have long been excluded from review under the APA. Even if such day-to-day operational decisions are "agency action" within the meaning of the APA, they lack any of the established features of *finality*—they do not create any rights or obligations, nor do any legal consequences flow from them.

C. Even if plaintiffs could overcome these threshold barriers to the adjudication of their claims, they are not likely to prevail on the merits. The Privacy Act specifically authorizes disclosure of records containing personal information to "those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." 5 U.S.C. § 552a(b)(1). The disclosure of plaintiffs' records to DOGE team members employed by the agency falls squarely within that authorization. The DOGE team members targeted by plaintiffs' complaint are SSA employees who "need" to access SSA data systems to perform their vital efforts to modernize those systems and to "[m]aximize [e]fficiency and [p]roductivity" of agency records, software, and information technology as directed by the President's Executive Order 14,158, including through the rooting out of

fraud, waste, and abuse in government programs. As the district court recognized and plaintiffs do not dispute, other agency employees performing similar functions have long had administrative access to these exact same agency systems and the personal information they contain. The district court provided no basis in law for second-guessing the Executive's determination that the DOGE team employees need access to those systems to perform their lawful functions.

II. The district court badly misjudged the remaining preliminary injunction factors. As numerous courts have recognized, plaintiffs suffer no harm, let alone irreparable harm, from the potential disclosure of their information to agency employees who are bound by law to maintain the information's confidentiality. By contrast, the district court's injunction imposes significant burdens on the Executive Branch. It usurps the President's prerogative to direct the proper functioning of the Executive Branch and undermines the public interest by thwarting the Executive's critically important efforts to improve the SSA's information-technology infrastructure and to eliminate waste, fraud, and abuse. The balance of equities thus weighs strongly against the district court's injunction.

## STANDARD OF REVIEW

This Court "review[s] the grant or denial of a preliminary injunction for abuse of discretion, recognizing that preliminary injunctions are extraordinary remedies involving the exercise of very far-reaching power to be granted only sparingly and in limited circumstances." *MicroStrategy Inc. v. Motorola, Inc.*, 245 F.3d 335, 339 (4th Cir. 2001) (quotation omitted). "A ruling that rests on an error of law is necessarily an abuse of discretion." *Pendleton v. Jividen*, 96 F.4th 652, 656 (4th Cir. 2024).

## ARGUMENT

Injunctive relief is an "extraordinary remedy that may only be awarded upon a clear showing that the plaintiff is entitled to such relief." *Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 22 (2008). To be entitled to a preliminary injunction, plaintiffs had to clearly show "that [they are] likely to succeed on the merits, that [they are] likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in [their] favor, and that an injunction is in the public interest." *Id.* at 20.

The district court abused its discretion in ruling that plaintiffs met this high standard. Its preliminary injunction should be vacated.

## I. Plaintiffs Have No Likelihood of Success on the Merits

Plaintiffs failed to demonstrate that they are likely to succeed on the merits of their claims. The district court granted broad injunctive relief that reconfigures the internal workings of a crucial government agency by dictating which agency employees can access agency data and under what conditions. That decision was error, for multiple reasons.

As a threshold matter, plaintiffs lack Article III standing because they do not suffer a cognizable harm based on *which* agency employees have access to their information contained in agency databases. Further, the agency's decisions about data access are not "final agency action" reviewable under the APA. And even if this case were justiciable, plaintiffs' claims are meritless because the Privacy Act authorizes employees to access their agency's systems of record when needed to perform their job duties, as is the case here.

Each issue above is independently fatal to plaintiffs' claims, and in the absence of a "clear showing" by plaintiffs that they are "likely to succeed" on *all* of them, *Winter*, 555 U.S. at 20, 22; *see AFT v. Bessent*,

No. 25-1282, 2025 WL 1023638, at *3 (4th Cir. Apr. 7, 2025) (Richardson, J., concurring), the preliminary injunction was an abuse of the district court's discretion.

### A. Plaintiffs suffer no cognizable Article III injury based on *which* SSA employees access agency data that plaintiffs voluntarily supplied to the agency

Article III standing is a "bedrock constitutional requirement that [the Supreme Court] has applied to all manner of important disputes." *United States v. Texas*, 599 U.S. 670, 675 (2023). It is "built on a single basic idea—the idea of separation of powers." *Id.* (quotation omitted). The requirement that plaintiffs demonstrate standing "helps safeguard the Judiciary's proper—and properly limited—role in our constitutional system," *id.* at 675–76, by ensuring that federal courts do not become "forums for the ventilation of public grievances" more properly resolved through the democratic process, *Valley Forge Christian Coll. v. Americans United for Separation of Church & State, Inc.*, 454 U.S. 464, 473 (1982).

To establish Article III standing, a plaintiff must demonstrate that he "has suffered or likely will suffer an injury in fact," *Food & Drug Admin. v. Alliance for Hippocratic Med.*, 602 U.S. 367, 380 (2024),

that is "legally and judicially cognizable," *Raines v. Byrd*, 521 U.S. 811, 819 (1997). The alleged injury must be "actual or imminent, not speculative," *Alliance for Hippocratic Med.*, 602 U.S. at 381, as well as "'concrete'—that is, 'real, and not abstract,'" *TransUnion LLC v. Ramirez*, 594 U.S. 413, 424 (2021) (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340 (2016)). Although "tangible" harms more readily qualify as concrete injuries, certain intangible harms can also be concrete. *Id.* at 425. "Central to assessing concreteness is whether the asserted harm has a 'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts." *Id.* at 417 (quoting *Spokeo*, 578 U.S. at 341).

Consequently, plaintiffs cannot satisfy Article III by alleging a bare statutory violation. Although Congress can create "a statutory prohibition or obligation and a cause of action," Article III still "requires a concrete injury even in the context of a statutory violation," and courts cannot "loosen Article III based on contemporary, evolving beliefs about what kinds of suits should be heard in federal courts." *TransUnion*, 594 U.S. at 425, 426.

An organization may establish standing by showing (in addition to other requirements) the standing of its members. *Hunt v. Washington State Apple Advert. Comm'n*, 432 U.S. 333, 343 (1977).

### 1. Plaintiffs cannot demonstrate a concrete injury-in-fact

Plaintiffs have not—and cannot—demonstrate that they or their members have suffered any concrete injury-in-fact. Instead, plaintiffs assert a purely intangible form of injury—namely, that the disclosure of their members' personal information to SSA employees who are DOGE team members (as opposed to other SSA employees who plaintiffs concede can lawfully access their members' data) constitutes an invasion of their members' privacy. (*See* JA39–42.) Thus, plaintiffs' alleged harm is the discomfort their members experience when *certain* SSA employees have access to their personal information. That alleged injury is not "concrete" under the standard set out in *TransUnion*.

Indeed, plaintiffs' alleged injury closely resembles the harms the Supreme Court deemed insufficiently concrete in *TransUnion*. There, the Court held that the mere fact that the defendant allegedly maintained inaccurate information about the plaintiffs within the company's internal files, in violation of a statutory requirement, failed

to establish standing. Even though the inaccurate information was quite serious—an alert indicating that the individual's name was a "potential match" to a name on a government list of "terrorists, drug traffickers, or other serious criminals"—any harm to the plaintiffs would become concrete only upon publication of the inaccurate information to third parties. *TransUnion*, 594 U.S. at 419–20, 434.

Here too, the mere fact that the government allegedly violated the Privacy Act by allowing certain SSA employees to access information stored in SSA databases does not alone demonstrate a concrete harm. After all, plaintiffs do not contend that their members' information has been shared with parties outside the government or others likely to misuse their information. To the contrary, SSA DOGE team members—like everyone else at the SSA—are bound by the same legal and ethical restrictions on the disclosure of plaintiffs' members' information, including the Privacy Act's authorization of criminal penalties for willfully engaging in prohibited disclosures, 5 U.S.C. § 552a(i)(1); *see id.* § 552a(g) (civil remedies against the agency), and the criminal penalties in the Social Security Act, 42 U.S.C. § 1306(a). Nor does plaintiffs' members' alleged "distress[]" at the thought of

certain SSA employees accessing their data suffice. *See* Order Denying Stay 20, Dkt. 20 (Richardson, J., dissenting). Plaintiffs' members voluntarily provided their information to the SSA and did so on the understanding that the information could be accessed by agency employees (and shared outside the agency) for any of the numerous purposes set forth in the Privacy Act and the agency's Statement of Records Notices. *See* 5 U.S.C. § 552a(b)(2)–(13); *infra* pp. 30–31. Thus, the mere fact that some additional SSA employees have access to databases containing plaintiffs' members' personal information does not harm plaintiffs' members in any concrete way.

### 2. Plaintiffs' alleged harm does not have a "close relationship" to intrusion upon seclusion

The district court nevertheless held that plaintiffs' alleged injury is analogous to the common-law tort of intrusion upon seclusion. (JA1347–1383.) That conclusion is wrong for several reasons.

To start, *TransUnion* requires a "close relationship" between the asserted common-law tort and the alleged statutory violation. 594 U.S. at 425. Although an "exact duplicate" is not required, plaintiffs' claimed injury must have a close common-law analog, and even relatively

modest distinctions foreclose standing. For that reason, the Court in *TransUnion* rejected the plaintiffs' fallback argument that the *internal* publication of information to "employees within TransUnion and to … vendors" constituted a concrete injury. *Id.* at 434 n.6. That argument was "unavailing" because "many American courts did not traditionally recognize intra-company disclosures" or those to vendors "as actionable publications for purposes of" the relevant analog—there, the common-law "tort of defamation." *Id.* The cases generally required "that the document was actually read," but that "evidence [was] lacking" in *TransUnion*. *Id.*

Here, plaintiffs' novel theory of injury under the Privacy Act bears no resemblance to the common-law tort of intrusion upon seclusion. As the district court acknowledged (JA1355), the Restatement (Second) of Torts § 652B (Am. Law Inst. 1977), Westlaw (database updated Oct. 2024), defines "intrusion upon seclusion" as an "intentional[] intru[sion], physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, … if the intrusion would be highly offensive to a reasonable person." *See also id.* § 652B cmt. a (describing the tort as "an intentional interference with" a person's

interest in "solitude or seclusion, either as to his person or as to his private affairs or concerns, of a kind that would be highly offensive to a reasonable man"). The Restatement provides examples that would meet that high standard, including "physical intrusion into … the plaintiff's room in a hotel" or his home; "use of the defendant's senses … to oversee or overhear the plaintiff's private affairs"; and "opening [the plaintiff's] private and personal mail [or] searching his safe or his wallet." *Id.* § 652B cmt. b. As these examples illustrate, the *sine qua non* of the common-law tort of intrusion upon seclusion is a highly offensive "intrusion into an individual's private space." *Bessent*, 2025 WL 1023638, at *2 (Agee, J., concurring); *see also O'Leary v. TrustedID, Inc.*, 60 F.4th 240, 246 (4th Cir. 2023) ("It's the unwanted intrusion into the home that marks intrusion upon seclusion.").

Plaintiffs' alleged injury in this case bears no resemblance to that kind of highly offensive intrusion into a person's private space. SSA personnel here are not surreptitiously invading plaintiffs' hotel rooms or monitoring their private communications. Instead, the SSA undisputedly obtained the personal information of plaintiffs' members legally, and it legally retains that information in data systems that are

maintained by the agency. Plaintiffs' alleged injury is thus "different in kind, not just in degree, from the harm inflicted" by snooping "reporters, detectives, and paparazzi." *See Bessent*, 2025 WL 1023638, at *5 (Richardson, J., concurring).

Moreover, plaintiffs do not dispute that their members' personal information can lawfully be accessed by employees of the SSA and shared outside the agency for any of the numerous purposes set forth in the Privacy Act and the agency's Statement of Records Notices. *See* 5 U.S.C. § 552a(b)(2)–(13). The agency's Statement of Records Notices permit even non-government personnel to access data "when they are performing work for us, as authorized by law, and they need access to personally identifiable information (PII) in our records in order to perform their assigned agency functions." *See* Privacy Act of 1974; System of Records, 87 Fed. Reg. 263, 265 (Jan. 4, 2022); Privacy Act of 1974, as Amended; New and Revised Privacy Act Systems of Records and Deletion of Obsolete Systems of Records, 71 Fed. Reg. 1796, 1831 (Jan. 11, 2006); Privacy Act of 1974, System of Records, 85 Fed. Reg. 2224, 2226 (Jan. 14, 2020); *see also* 20 C.F.R. § 401.115. Plaintiffs can hardly complain of a concrete injury when their members provided

personal information to a government agency on the understanding that it would be maintained on agency computer systems and used by agency employees and others for a variety of lawful purposes, including the investigation of improper payments—which is what the SSA's DOGE team members plan to do.

Neither the district court nor plaintiffs have offered any authority suggesting that the purely *internal* disclosure of personal information within an organization that is authorized to maintain and use that information would have been actionable at common law. That is not surprising, as the Restatement makes clear that such internal access and use of information was never contemplated by the common-law tort. Specifically, the notes to the Restatement explain that "locating and supplying information for one's own files is not an intrusion." Restatement (Second) of Torts § 652B, Reporter's Note (1977). And in support of that point, the Restatement cites the Eighth Circuit's decision in *Tureen v. Equifax, Inc.*, 571 F.2d 411, 416 (8th Cir. 1978), which presented analogous facts to those alleged here: the plaintiff alleged that Equifax had unlawfully prepared a report about the plaintiff's claim history based on credit report information maintained

in Equifax's records. *Id.* at 413–14. In rejecting the plaintiff's theory of intrusion upon seclusion, the Eighth Circuit explained that it was critical that the defendant "obtained the information about which plaintiff complains merely by means of searching defendant's own files containing a summary of defendant's own prior reports on plaintiff." *Id.* at 415. That was "hardly an act which intruded in any manner upon plaintiff." *Id.* Because there, as here, the plaintiff had no basis to challenge the collection and retention of his information, there was no violation of any recognized privacy interest. *Id.*

Other courts confronting similar facts have consistently followed the Restatement's admonition to conclude that such internal reviews are not the kind of highly objectionable intrusion contemplated by the tort of intrusion upon seclusion. *See, e.g.*, *In re Trans Union Corp., Priv. Litig.*, 326 F. Supp. 2d 893, 902 (N.D. Ill. 2004) ("Trans Union's accessing its own lawfully obtained files cannot be considered an unlawful intrusion."); *Miller v. Motorola, Inc.,* 560 N.E.2d 900 (Ill. App. Ct. 1990) (accessing information voluntarily provided to defendant does not amount to unauthorized intrusion).

Plaintiffs' theory of injury is different in kind from that recognized at common law in yet another respect: the tort of intrusion upon seclusion "guards against the unease of having one's 'private concerns' *specifically* targeted by another's 'investigation or examination.'" Order Denying Stay 19, Dkt. 20 (Richardson, J., dissenting) (emphasis added) (quoting Restatement (Second) of Torts § 652B cmt. b). "The tort addresses narrow, individualized scrutiny—not general, impersonal oversight." *Id.* Yet plaintiffs do not allege "that they have been the subject of any targeted snooping"; nor do they even allege that any "DOGE-affiliated SSA employee has seen their specific personal information." *Id.* at 20. Plaintiffs would have no reason to suspect that any particular SSA employee has accessed any of their member's information in the normal course of that employee's duties. *See TransUnion*, 594 U.S. at 438 (certain plaintiffs had not suffered an injury sufficient to support standing where they did not "even *kn*[*o*]*w*" their files contained inaccurate information).

At bottom, plaintiffs' members' distress at the knowledge that particular SSA employees have access to SSA databases containing their members' voluntarily-supplied information does not amount to a

concrete injury. *Cf. Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 418 (2013) (holding that "self-inflicted injuries are not fairly traceable to the Government's purported activities"). Far from constituting a highly objectionable invasion of personal privacy, SSA DOGE team members who may access plaintiffs' members' information are doing the same thing that other agency employees routinely and properly do. That is no injury at all, let alone a cognizable Article III injury.

### 3. The district court misconstrued this Court's precedents

In concluding otherwise, the district court misconstrued this Court's decisions in *O'Leary v. TrustedID, Inc.*, 60 F.4th 240 (2023), *Garey v. James S. Farrin, P.C.*, 35 F.4th 917 (2022), and *Krakauer v. Dish Network, LLC*, 925 F.3d 643 (2019), which confirm that intrusion into an individual's private space is an essential element of the common-law tort of intrusion upon seclusion and that mere access to a person's voluntarily-provided information, as in this case, is insufficient.

In *Krakauer*, the plaintiff alleged he was harmed when a telemarketer "disregard[ed] the [Do Not Call] registry and actually place[d] multiple calls" to the plaintiff's home. 925 F.3d at 654. Citing

the Restatement, the Court concluded that the phone calls represented a "cognizable intrusion[]" upon the plaintiff's seclusion by burdening the plaintiff's "long protected privacy interests in the home." *Id.* at 653. Similarly, the plaintiffs in *Garey* sued attorneys who had obtained their names and addresses from public car accident reports and used that personal information to mail unsolicited advertising materials to the plaintiffs' homes. 35 F.4th at 919–20. This Court described the *Garey* plaintiffs' theory of standing, based on an alleged invasion of privacy, as being "nearly identical" to that raised by the plaintiffs in *Krakauer*. *Id.* at 921–22. Emphasizing "the right of the plaintiff … to be let alone," the Court held that the plaintiffs in *Garey* had alleged a legally cognizable privacy injury for Article III standing purposes. *Id.* at 922 (quotation omitted).

Crucially, both *Krakauer* and *Garey* involved "some sort of interjection into the [individual's] private sphere," *Bessent*, 2025 WL 1023638, at *2 (Agee, J., concurring)—unwanted telemarketing calls to the individual's residence in *Krakauer* and unsolicited advertising materials mailed to the individual's home in *Garey*.

By contrast, this Court found the injury alleged in *O'Leary*, 60 F.4th 240, to be insufficient to satisfy Article III because it lacked the defining feature of the common-law tort. There, the credit reporting agency Equifax was the subject of a data breach, and it engaged its subsidiary, TrustedID, to inform customers whether their information had been compromised in the data breach. O'Leary provided six digits of his social security number to TrustedID, through its website, in exchange for learning whether he was impacted, upon which he was informed that he was not impacted. O'Leary then filed an action in state court alleging that TrustedID's practice of requiring six digits of a consumer's social security number on its website, without using other security precautions, violated state law. O'Leary also alleged that TrustedID had shared his partial social security number with Equifax. Equifax removed the case to federal court under the Class Action Fairness Act and moved to dismiss. Addressing its jurisdiction, the district court held that O'Leary had asserted "an intangible concrete harm in the manner of an invasion of privacy" that satisfied Article III standing, but it nonetheless proceeded to dismiss the case on the merits. *Id.* at 242 (emphasis and quotation omitted).

This Court vacated the district court's decision, finding subject matter jurisdiction lacking because O'Leary had "alleged only a bare statutory violation and no Article III injury." *O'Leary*, 60 F.4th at 242. On the question "whether O'Leary suffered a concrete injury in fact," *id.*, the Court found instructive its data-breach precedents holding that "being subjected to a data breach isn't in and of itself sufficient to establish Article III standing without a nonspeculative, increased risk of identity theft," *id.* at 244. The Court explained that "Article III excludes plaintiffs who rely on an abstract statutory privacy injury unless it came with a nonspeculative increased risk of identity theft." *Id.*[4]

Nor had O'Leary alleged an injury with a "'close relationship' to a traditional or common-law analog" as *TransUnion* requires. *O'Leary*, 60 F.4th at 245. As for O'Leary's alleged injury based on his "privacy interest in his Social Security number," this Court held that "such an injury bears no close relationship to a traditional or common-law

[4] The district court in this case properly rejected plaintiffs' alleged injury-in-fact that their members faced "exposure to an increased and non-speculative risk of identity theft" as a result of the SSA DOGE team members' access to their data in SSA databases. (JA1353.)

analog," including the tort of "intrusion upon seclusion." *Id.* (quotation omitted). Unlike the situation in *Krakauer* involving "unwanted calls," O'Leary "*chose* to hand over his partial [social security number] 'in exchange for' finding out whether he was impacted by Equifax's data breach." *Id.* at 245–46 (emphasis added, alteration omitted). Far from an "unwanted intrusion into the home that marks intrusion upon seclusion," O'Leary had not pleaded "anything that closely relates to that." *Id.* at 246.

So too here. Plaintiffs' members in this case chose to provide their personal information to SSA in exchange for government benefits and with the understanding that their information could be accessed by SSA employees for a variety of purposes. The purported injury to their abstract privacy interest in that information, based on *which* SSA employees can access their data, has no resemblance to the kind of unwanted and highly offensive intrusion that animates the common-law tort of intrusion upon seclusion.

The district court tried to distinguish *O'Leary* on the theory that "this case concerns far more than access to even complete SSNs [social security numbers]" and "involves access to a wide swath of confidential

and sensitive PII [personally identifiable information]." (JA1361.) But this Court's analysis in *O'Leary* did not turn on the amount or degree of sensitivity of the underlying information in which a privacy interest was claimed. As this Court said in *Krakauer*, the proper inquiry "is focused on the *types* of harms protected at common law, not the precise point at which those harms become actionable." 925 F.3d at 654 (emphasis added). Thus, the *O'Leary* Court did not question the sensitivity and confidential nature of the information at issue there, but focused instead on the type of harm alleged, and it concluded that "O'Leary [had not] alleged an injury with a close relationship to 'intrusion upon seclusion.'" 60 F.4th at 245.

The district court also relied on two decisions from other circuits holding that plaintiffs alleging violations of the Fair Credit Reporting Act had Article III standing to pursue their claims. (JA1367–1369.) *See Persinger v. Southwest Credit Sys., L.P.*, 20 4th 1184 (7th Cir. 2021); *Nayab v. Capital One Bank (USA), N.A.*, 942 F.3d 480 (9th Cir. 2019). The plaintiffs in those cases alleged a privacy harm arising from the defendants' actions in unlawfully obtaining and using their credit information, but the plaintiffs did not provide their information to the

defendants, as plaintiffs did here, and the defendants in those cases did not lawfully obtain and maintain the information at issue, like SSA did and does here. Neither decision supports the district court's ruling in this case.

In sum, without a common-law analog to their alleged injury in this case, plaintiffs cannot establish an injury-in-fact and, therefore, lack standing to pursue their claims. The district court's preliminary injunction should be vacated on that ground alone.

### B. Plaintiffs do not challenge any final agency action reviewable under the APA

The district court additionally lacked authority to adjudicate plaintiffs' claims because only "final agency action" is reviewable under the APA, 5 U.S.C. § 704, and an agency's decisions as to which of its employees may access particular agency data do not qualify.

It is well settled that not all agency conduct is subject to review under the APA. As the Supreme Court has explained, the APA does not permit "general judicial review of [an agency's] day-to-day operations." *Lujan v. National Wildlife Fed'n*, 497 U.S. 871, 899 (1990). Nor does the APA authorize courts to oversee "the common business of managing

government programs." *Fund for Animals, Inc. v. U.S. Bureau of Land Mgmt.*, 460 F.3d 13, 20 (D.C. Cir. 2006).

Plaintiffs' complaint seeks review of exactly that kind of day-to-day management of agency operations. The supposed "agency action" plaintiffs identify is a loosely defined series of personnel decisions related to granting individual employees access to agency systems. Plaintiffs contend that SSA granted access to DOGE team members too quickly and without adequately vetting those employees, providing them with sufficient training, or correctly assessing their need for access to SSA systems.[5] As *Lujan* held, such day-to-day decisions and conduct fall outside the APA's ambit. *See* 497 U.S. at 899. This Court has likewise recognized that courts "are woefully ill-suited … to adjudicate" "attack[s]" "asking [the judiciary] to improve an agency's

[5] The district court concluded that three members of the DOGE team "were not properly detailed to SSA" and "were not entitled to access" because their "necessary work documents were not signed" at the time access was first granted to them. (JA1401.) Of those three, one's onboarding agreement was not finalized until the day after access was granted; another's not until 10 days after; and the third's purportedly "remain[ed] unsigned," according to the court (JA1401). (*But see* JA402 (SSA declaration stating that the last of these three (Employee 8) has a "fully signed and completed" onboarding agreement).) In any event, no such minor issues existed for any of the other DOGE team members, and the district court found none.

performance or operations." *City of New York v. U.S. Dep't of Def.*, 913 F.3d 423, 431 (4th Cir. 2019) (quotation omitted). In that kind of case, "courts would be forced either to enter a disfavored 'obey the law' injunction or to engage in day-to-day oversight of the executive's administrative practices. Both alternatives are foreclosed by the APA, and rightly so." *Id.* (citation omitted).

Indeed, plaintiffs' and the district court's understanding of what qualifies as "agency action" would have sweeping and untenable consequences. Agencies make thousands of personnel decisions every day of the type plaintiffs challenge here, whether by creating an e-mail account for an employee, staffing an employee on a particular matter, or ensuring that an employee has the relevant training and credentials to access systems or participate in programs. If courts can review such decisions, virtually every aspect of an agency's internal management of its employees could trigger APA review—a result that no courts have countenanced until now.

Far from identifying relevant precedents for such review, the district court simply stated that the "approval decisions are akin to a binding agency opinion—one that established DOGE's entitlement to

access [personally identifiable information] notwithstanding the Agency's customs, practices, policies, and procedures." (JA1402.) But the fact that an agency decision (in the court's view) differs from prior decisions does not make it a reviewable agency action.

Even if SSA's decisions to grant certain employees access to agency databases qualify as "agency action," they are not "final" for purposes of the APA. Such decisions are not actions through which "rights or obligations have been determined" or from which "legal consequences will flow," *Bennett v. Spear*, 520 U.S. 154, 177–78 (1997); *see also U.S. Army Corps of Eng'rs v. Hawkes Co.*, 578 U.S. 590, 597 (2016), and plaintiffs failed to demonstrate how providing employees with system access meets any of those criteria. There is no final agency action where the challenged act "impose[d] no obligations, prohibitions or restrictions on regulated entities" and "d[id] not subject them to new penalties or enforcement risks." *Sierra Club v. EPA*, 955 F.3d 56, 63 (D.C. Cir. 2020). Plaintiffs are not regulated by internal agency decisions to allow new employees access to the agency's systems, nor have they identified any direct legal consequences that arise from those decisions, which may change or be adjusted at any time.

Even if such decisions could produce indirect, practical consequences for plaintiffs, they would not be final agency action. Adverse effects "accompany many forms of indisputably non-final government action." *Air Brake Sys., Inc. v. Mineta*, 357 F.3d 632, 645 (6th Cir. 2004). For example, "initiating an enforcement proceeding against a company … may have a devastating effect on the company's business, but that does not make the agency's action final." *Id.* What matters is that the alleged data access decisions here have no "direct and appreciable legal consequences" for plaintiffs. *California Cmtys. Against Toxics v. EPA*, 934 F.3d 627, 640 (D.C. Cir. 2019). That forecloses plaintiffs' APA claim.

Plaintiffs cannot avoid that conclusion by claiming they target some broader "policy" capable of APA review. In concluding otherwise, the district court relied on a single out-of-circuit precedent, *Venetian Casino Resort, LLC v. EEOC*, 530 F.3d 925 (D.C. Cir. 2008), that is not analogous to this case. (JA1402–1403.) In *Venetian*, the D.C. Circuit held that the Equal Employment Opportunity Commission's (EEOC) policy of disclosing an employer's confidential information (possibly including trade secrets) to third parties who were potential plaintiffs

with discrimination claims against the employer constituted final agency action. Unlike this case, the EEOC's disclosure policy was memorialized in multiple versions of the agency's compliance manual, and the agency's disclosures of the employer's confidential trade secret information to third parties, once accomplished, would have immediate material consequences for the employer. By contrast, this case involves data access within an agency, not third-party disclosures. Review of data contained in internal agency systems by agency employees is different in kind and does not threaten any comparable harms. *See City of New York*, 913 F.3d at 431 ("a party must demonstrate that the challenged act had an immediate and practical impact or altered the legal regime in which it operates") (quotations and brackets omitted); *cf. Hunstein v. Preferred Collection & Mgmt. Servs., Inc.*, 48 F.4th 1236, 1240, 1245–50 (11th Cir. 2022) (en banc) (explaining that without third-party disclosure, claims founded on internal disclosure of data do not state a cognizable injury for standing purposes); *see supra* pp. 27–28 (discussing *TransUnion*'s rejection of an internal-disclosure theory of standing).

### C. Plaintiffs' Privacy Act and APA claims fail on the merits

Even if plaintiffs' claims were justiciable, they would fail on the merits. The district court addressed only two of those claims: (1) that "SSA's provision to the DOGE Team of access to SSA systems is 'not in accordance with'" law—*i.e.*, the Privacy Act—because defendants had failed to establish the employees' need to access the relevant databases, and (2) that defendants' failure to establish the DOGE employees' need rendered the decision to grant them access unreasonable, in violation of the APA. (JA1435–1436.) Those related holdings are both erroneous.

#### 1. Privacy Act claim

While the Privacy Act generally prohibits disclosure of covered records containing personal information absent consent, 5 U.S.C. § 552a(b), it contains several exceptions, *id.* § 552a(b)(1)–(13). Relevant here, the statute expressly authorizes disclosure to "those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." *Id.* § 552a(b)(1). That language makes clear that the "need" exception applies "to intra-agency disclosures." *Britt v. Naval Investigative Serv.*, 886 F.2d 544, 547 (3d

Cir. 1989). The disclosure of plaintiffs' records to DOGE team members within the SSA falls squarely within that authorization.

a. First, the relevant DOGE team members are employees of SSA for Privacy Act purposes. "For the purpose of" Title 5 of the U.S. Code—which includes the Privacy Act—"employee" means "an officer and an individual who is" first "appointed in the civil service by," *inter alia*, "the President" or "an individual who is an employee under this section." 5 U.S.C. § 2105(a)(1)(A), (D). An employee must also be "engaged in the performance of a Federal function under authority of law or an Executive act" and "subject to the supervision of an individual named by paragraph (1) of this subsection while engaged in the performance of the duties of his position." *Id.* § 2105(a)(2), (3). The SSA DOGE team members satisfy that definition, and the district court did not hold otherwise. (*See* JA1416 (assuming that the relevant team members "have 'intra agency' status at SSA")); *see also* Exec. Order No. 14,158 § 3(c), 90 Fed. Reg. 8441 (directing agency heads to "establish within their respective Agencies a DOGE Team of at least four employees").

Second, the SSA DOGE team members have a "need" to access the records contained in the relevant systems to perform their official duties. 5 U.S.C. § 552a(b)(1). "Need" exists if "the official examined the record in connection with the performance of duties assigned to him and [if] he had to do so in order to perform those duties properly." *Bigelow v. Department of Def.*, 217 F.3d 875, 877 (D.C. Cir. 2000), *cert. denied*, 532 U.S. 971 (2001).

That standard is met here. The DOGE team at SSA has been established to "moderniz[e] Federal technology and software to maximize governmental efficiency and productivity." Exec. Order No. 14,158, § 1, 90 Fed. Reg. 8441; *see id.* § 4. Specifically, the Executive Order directed the undertaking of a "Software Modernization Initiative to improve the quality and efficiency of government-wide software, network infrastructure, and information technology … systems," and it requires agency heads to work with USDS to "promote inter-operability between agency networks and systems, ensure data integrity, and facilitate responsible data collection and synchronization." *Id.* § 4(a). Consistent with that effort, the Executive Order instructs agency heads "to the maximum extent consistent with law, to ensure USDS has full

and prompt access to all unclassified agency records, software systems, and IT systems," and in turn requires USDS to "adhere to rigorous data protection standards." *Id.* § 4(b). In compliance with this directive, SSA provided a limited number of its SSA DOGE team members access to agency data needed for projects focused on such modernization, data integrity, and efficiency.

The Executive Order thus necessitates that agency personnel working to implement its directives have access to records and systems of records under the Privacy Act to assess the state of the systems and to "improve the[ir] quality and efficiency." Exec. Order No. 14,158, § 4(a), 90 Fed. Reg. 8441; *see Bigelow*, 217 F.3d at 877. Indeed, it is difficult to imagine how agency personnel seeking to modernize agency systems could do so *without* access to the systems themselves.

The "need" for such access was substantiated by the DOGE team members' various requests for access to SSA systems. (*See* JA542–573.) As one example, a February 19, 2025, memorandum from SSA's Chief Information Officer to SSA's Acting Commissioner explained that certain DOGE team members required access to certain SSA master

records and payment files containing personally identifiable information. (JA546–549.) The Chief Information Officer explained—

> SSA has a need to rapidly respond to concerns regarding potentially large-scale fraud and improper payments related to data issues in payment files SSA sends to BFS and concerns that those potential issues in those payment files may relate, in part, to SSNs without an associated date of death in SSA's Numident master files.

(JA546.) He further explained that the DOGE team members requiring access have "the skills and abilities to conduct the requisite data analysis and review to address [those] concerns" and that "this task is within their currently-assigned job duties." (JA546.) He concluded that their access to personally identifiable information would also be necessary for the task:

> We investigated options for masked or otherwise protecting PII-containing [personally identifiable information] and FTI-containing [federal tax information] fields within these records but have not identified a solution that enables the necessary analysis to continue at the pace necessary to respond timely to the fraud and improper-payment-related concerns.

(JA546.) As another example, an email exchange and accompanying memorandum dated February 28, 2025, describe the DOGE team's plans to improve the death data maintained in SSA's Numident files to prevent government payments from being improperly issued to

deceased individuals, and those efforts would require access to SSA systems. (JA550–559.) Another request, dated March 14, 2025, explained that "select access" to a certain SSA system with "identifying information about beneficiaries and their application documents" was needed "as part of [the requestor's] duties as a senior advisor for the SSA" who was "investigating fraud, waste, and abuse and improper payments." (JA560–561.) And another request, dated March 19, 2025, sought access to certain systems with data about "when users log into MySSA, Call the 1-800 Number, Call the Field office, [or] have an appointment in the field offices" so that the requestor could "build a system to analyze how often beneficiaries interact with the SSA in order to identify users that may be dead and receiving benefits." (JA562.)

The list goes on: statements of need for access accompanied additional requests dated March 12, March 14, March 15, March 17, and March 18, 2025. (*See* JA564–573.) In addition, SSA declarations submitted in the district court also describe the projects assigned to DOGE team members at SSA and why access to personally identifiable

information, without anonymization, is necessary to accomplish them. (JA113–119, JA396–400, JA453–456, JA458–460; *see also* JA518–526.)[6]

Clearly, DOGE team members investigating whether the government has made improper expenditures require access to the records detailing the relevant payments. To assess the propriety of any payment, an analyst needs to know the details surrounding that payment, including information about the recipient of that payment, the amount of the payment, the payment's purpose, and so forth. It is hard to fathom how such investigative work could be performed without access to the relevant payment records. Indeed, the President has expressly directed agency heads to ensure that "Federal officials designated by the President or Agency Heads (or their designees) have full and prompt access to all unclassified agency records, data, software systems, and information technology systems" in order to combat fraud,

[6] Defendants dispute the district court's characterization of these declarations as providing "post hoc explanations for 'need.'" (JA1428.) To the contrary, the need for access set forth in the SSA DOGE team's various requests was readily apparent to those already familiar with the SSA's systems and the DOGE team's various projects, including to the SSA's Acting Commissioner who approved the access. The purpose of the declarations was to help educate the district judge about the SSA's systems and the DOGE team's various projects, not to provide post hoc explanations for need.

waste, and abuse. Exec. Order No. 14,243, § 3, 90 Fed. Reg. 13,681 (Mar. 25, 2025).

b. The district court's contrary determination stemmed in significant part from its view that the scope of disclosure in this case is larger than in prior Privacy Act disputes. (JA1416 (noting that Privacy Act cases "typically involve the disclosure of records concerning a single person or a small number of people").) But it is hardly surprising—much less legally relevant—that employees would "need" to access more records to modernize the government's information systems and detect systemic fraud than would be necessary in a one-off case concerning the government's investigation into, for example, allegations against a particular employee. *See, e.g.*, *Bigelow*, 217 F.3d at 370–71. Here, a limited number of SSA DOGE team members have been granted access to information for specific purposes that require that access. The Privacy Act does not authorize the district court to micromanage that lawful access.

Moreover, although the district court purported to exempt non-DOGE activity from its preliminary injunction (*see* JA1296), the court's reasoning would apparently call into doubt the legality of the SSA's

granting of access to the many non-DOGE employees who have had access to the relevant systems for years and who have been performing tasks substantially similar to the work being performed by DOGE team members. The only apparent difference is that the district court approves of the non-DOGE-related agency employees' activity, but it disapproves of the activities of DOGE. That is the kind of policy judgment that the Constitution vests in the Executive, not the Judiciary.

Much of the district court's analysis focused on whether defendants demonstrated that, beyond needing access to the records contained in the relevant systems, the SSA DOGE team *also* needed access to the personal information contained in those records. (*See* JA1427–1433.) But that distinction has no basis in the text of the Privacy Act. The statute allows employees to access a "record" if they have "a need for the record in the performance of their duties," 5 U.S.C. § 552a(b)(1), and it defines "record" as "any item, collection, or grouping of information about an individual … that contains his name" or other personally identifiable information. *Id.* § 552a(a)(4). In other words, the statutory question is whether the employee needs access to the

*record* as a whole—not the personally identifiable information it contains. A contrary rule would be entirely unworkable: it would require redaction review of every record and anonymization of certain fields within a record before any employee could do even the most basic tasks required by his job.

In any event, it is obvious that SSA employees who are, for example, tasked with investigating whether the government has made improper expenditures would need access to records detailing the relevant payments—including personally identifiable information like the recipient of the payment and its purpose—to determine (among other things) whether duplicative payments were made. Moreover, the administrative record and defendants' declarations explained that although the agency "investigated options for mask[ing] or otherwise protecting" personally identifiable information within records, it had not "identified a solution that enables the necessary analysis to continue at the pace necessary to respond timely to the fraud and improper-payment-related concerns." (JA546.) The district court found this explanation insufficient, on the theory that "it suggests only that working without" personally identifiable information "may cause the

[agency's] work to take longer." (JA1427.) But nothing in the Privacy Act permits the district court to substitute its own judgment regarding the speed required for crucial government work for that of the agency.

**2. APA claim**

The district court also erred in holding that plaintiffs are likely to succeed on their claim that defendants violated the APA by acting arbitrarily and capriciously. Review under the APA is "highly deferential, with a presumption in favor of finding the agency action valid." *Ohio Valley Env't Coal v. Aracoma Coal Co.*, 556 F.3d 177, 192 (4th Cir. 2009) (quotation omitted). Moreover, "the ultimate standard of review is a narrow one," as "the court is not empowered to substitute its judgment for that of the agency." *Id.*

The district court reasoned that "defendants have not provided the Court with a reasonable explanation for why the entire DOGE Team needs full access to the wide swath of data maintained in SSA systems in order to undertake the projects." (JA1435.) But as already discussed *supra* pp. 49–52, the government *did* provide such an explanation; and in any event, as Judge Richardson explained in *Bessent*, "it does not stretch the imagination to think that modernizing an agency's software

and IT systems would require administrator-level access to those systems, including any internal databases." 2025 WL 1023638, at *6 (Richardson, J., concurring). Once again, the district court's contrary determination simply substitutes its own views of agency best practices for the agency's determination that agency personnel tasked with modernizing the agency's data systems and ferreting out fraud, waste, and abuse need access to those systems.

## II. Plaintiffs Also Failed to Establish the Remaining Preliminary Injunction Factors

The remaining preliminary injunction factors—irreparable harm, the balance of equities, and the public interest—likewise favor the government. *See Mountain Valley Pipeline, LLC v. Western Pocahontas Props. Ltd. P'ship*, 918 F.3d 353, 366 (4th Cir. 2019) (Each of [the] four [preliminary injunction] requirements must be satisfied.").

First, plaintiffs cannot establish a cognizable injury for Article III standing purposes, let alone the kind of irreparable harm necessary to support a preliminary injunction. Plaintiffs cannot make a clear showing of irreparable harm from the SSA's intra-agency disclosure of information where the SSA DOGE employees who view that information are subject to the same confidentiality obligations that

apply to other agency employees. In finding that plaintiffs would suffer irreparable harm absent an injunction, the district court did not suggest that plaintiffs had demonstrated any risk that the SSA defendants or DOGE team members would further disseminate or misuse the relevant data. Rather, the mere fact that certain employees would continue to have access to information plaintiffs' members gave to the SSA was sufficient, in the district court's view, to support the extraordinary relief of a preliminary injunction. (JA1436–1440.)

That is plainly incorrect. As discussed, this Court in *Bessent* and three other district courts addressing similar claims have recognized that similarly situated plaintiffs lack irreparable harm. *See Bessent*, 2025 WL 1023638, at *6–7 (Richardson, J., concurring); *University of Cal. Student Ass'n v. Carter*, 766 F. Supp. 3d 114, 121–22 (D.D.C. 2025); *Electronic Privacy Info. Ctr. v. U.S. Office of Pers. Mgmt.*, No. 25-cv-255, 2025 WL 580596, at *6–7 (E.D. Va. Feb. 21, 2025); *Alliance for Retired Ams. v. Bessent*, No. 25-cv-313, 2025 WL 740401, at *20–24 (D.D.C. Mar. 7, 2025). As these courts have explained, "dissemination of information" may constitute "an irreparable injury where, for example, highly sensitive information will be made *public*, or ends up in the

hands of someone with no obligation to keep it confidential." *University of Cal. Student Ass'n*, 766 F. Supp. 3d at 121 (collecting authorities); *see Bessent*, 2025 WL 1023638, at *6–7 (Richardson, J., concurring). But dissemination of information does not constitute irreparable harm "where the challenged disclosure is not 'public,' but involves individuals obligated to keep it confidential." *University of Cal. Student Ass'n*, 766 F. Supp. 3d at 121.

That is the case here: SSA employees, including DOGE team members, "are obligated to use" the data "for lawful purposes … and to keep it confidential, in accordance with the Privacy Act" and other federal laws. *University of Cal. Student Ass'n*, 766 F. Supp. 3d at 122; *see Bessent*, 2025 WL 1023638, at *7 (Richardson, J., concurring); *Alliance for Retired Ams.*, 2025 WL 740401, at *21 (explaining that unlawful access does not constitute irreparable injury where the employee is bound to keep information confidential, because, if necessary, "a court can fashion 'adequate … corrective relief after the fact") (citation omitted).

As for the remaining factors, allowing the injunction to stand threatens irreparable injuries to the government and the public, whose

interests "merge" in this context. *Nken v. Holder*, 556 U.S. 418, 435 (2009). The injunction here impinges on the President's and the agency head's broad authority over and responsibility for directing employees in important work to modernize federal government systems and identify fraud, waste, and abuse throughout the federal government. It is therefore "an improper intrusion by a federal court into the workings of a coordinate branch of the Government." *Immigration & Naturalization Serv. v. Legalization Assistance Project of the L.A. Cty. Fed'n of Labor*, 510 U.S. 1301, 1306 (1993) (O'Connor, J., in chambers).

At every turn, the injunction inflicts irreparable constitutional harm. It erodes the President's control over subordinates and countermands his specific directions to agency heads. It frustrates the public's interest in having their elected President effectuate policy priorities—including ensuring tax dollars are not wasted on outdated systems or improper or fraudulent payments—through lawful direction of the Executive Branch. And it inserts the Judicial Branch into the day-to-day, internal operations of a federal agency.

## CONCLUSION

For the foregoing reasons, this Court should vacate the preliminary injunction.

Respectfully submitted,

YAAKOV M. ROTH
*Acting Assistant Attorney General*

ERIC D. MCARTHUR
*Deputy Assistant Attorney General*

GERARD SINZDAK
JACK STARCHER
SIMON JEROME

*s/ Jacob Christensen*
JACOB CHRISTENSEN
*Attorneys, Appellate Staff*
*Civil Division, Room 7525*
*U.S. Department of Justice*
*950 Pennsylvania Avenue NW*
*Washington, DC 20530*
*(202) 514-5048*
*jacob.christensen@usdoj.gov*

June 2025

## CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limit of Federal Rule of Appellate Procedure 32(a)(7)(B) because it contains 11,457 words. This brief also complies with the typeface and type-style requirements of Federal Rule of Appellate Procedure 32(a)(5)-(6) because it was prepared using Word for Microsoft 365 in Century Schoolbook 14-point font, a proportionally spaced typeface.

*s/ Jacob Christensen*
Jacob Christensen

**CERTIFICATE OF SERVICE**

I certify that on June 9, 2025, I electronically filed the foregoing brief with the Clerk of the Court for the United States Court of Appeals for the Fourth Circuit by using the appellate CM/ECF system. Service will be accomplished by the appellate CM/ECF system.

*s/ Jacob Christensen*
Jacob Christensen

# ADDENDUM

# TABLE OF CONTENTS

**The Privacy Act of 1974 - 5 U.S.C. § 552a**

**§ 552a. Records maintained on individuals**

***

**(b) Conditions of disclosure.**--No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be--

**(1)** to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;

***

**(3)** for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;

***

**(7)** to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;

***

**(e) Agency requirements.**--Each agency that maintains a system of records shall--

**(1)** maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President;

***

**(4)** subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include--

**(A)** the name and location of the system;

**(B)** the categories of individuals on whom records are maintained in the system;

**(C)** the categories of records maintained in the system;

**(D)** each routine use of the records contained in the system, including the categories of users and the purpose of such use;

**(E)** the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

**(F)** the title and business address of the agency official who is responsible for the system of records;

**(G)** the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;

**(H)** the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and

**(I)** the categories of sources of records in the system;

***

**(g)(1) Civil remedies.**--Whenever any agency

**(A)** makes a determination under subsection (d)(3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection;

**(B)** refuses to comply with an individual request under subsection (d)(1) of this section;

**(C)** fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to

assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual; or

**(D)** fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual,

the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.

***

**(i)(1) Criminal penalties.**--Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

**(2)** Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000.

**(3)** Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

***

**Administrative Procedure Act - 5 U.S.C. § 500 et seq.**

**§ 500. Definitions**

For the purpose of this subchapter--

***

(6) "order" means the whole or a part of a final disposition, whether affirmative, negative, injunctive, or declaratory in form, of an agency in a matter other than rule making but including licensing;

***

(13) "agency action" includes the whole or a part of an agency rule, order, license, sanction, relief, or the equivalent or denial thereof, or failure to act;

***

**§ 704. Actions reviewable**

Agency action made reviewable by statute and final agency action for which there is no other adequate remedy in a court are subject to judicial review. A preliminary, procedural, or intermediate agency action or ruling not directly reviewable is subject to review on the review of the final agency action. Except as otherwise expressly required by statute, agency action otherwise final is final for the purposes of this section whether or not there has been presented or determined an application for a declaratory order, for any form of reconsideration, or, unless the agency otherwise requires by rule and provides that the action meanwhile is inoperative, for an appeal to superior agency authority.

***

**§ 706. Scope of review**

To the extent necessary to decision and when presented, the reviewing court shall decide all relevant questions of law, interpret constitutional and statutory provisions, and determine the meaning or applicability of the terms of an agency action. The reviewing court shall--

***

(2) hold unlawful and set aside agency action, findings, and conclusions found to be--

(A) arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law;

(B) contrary to constitutional right, power, privilege, or immunity;

(C) in excess of statutory jurisdiction, authority, or limitations, or short of statutory right;

***

In making the foregoing determinations, the court shall review the whole record or those parts of it cited by a party, and due account shall be taken of the rule of prejudicial error.

**Establishing and Implementing the President's "Department of Government Efficiency" - Exec. Order No. 14158, 90 Fed. Reg. 8441 (Jan. 29, 2025)**

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered:

Section 1. Purpose. This Executive Order establishes the Department of Government Efficiency to implement the President's DOGE Agenda, by modernizing Federal technology and software to maximize governmental efficiency and productivity.

Sec. 2. Definitions. As used in this order:

(a) "Agency" has the meaning given to it in section 551 of title 5, United States Code, except that such term does not include the Executive Office of the President or any components thereof.

(b) "Agency Head" means the highest-ranking official of an agency, such as the Secretary, Administrator, Chairman, or Director, unless otherwise specified in this order.

Sec. 3. DOGE Structure. (a) Reorganization and Renaming of the United States Digital Service. The United States Digital Service is hereby publicly renamed as the United States DOGE Service (USDS) and shall be established in the Executive Office of the President.

(b) Establishment of a Temporary Organization. There shall be a USDS Administrator established in the Executive Office of the President who shall report to the White House Chief of Staff. There is further established within USDS, in accordance with section 31611 of title 5, United States Code, a temporary organization known as "the U.S. DOGE Service Temporary Organization". The U.S. DOGE Service Temporary Organization shall be headed by the USDS Administrator and shall be dedicated to advancing the President's 18-month DOGE agenda. The U.S. DOGE Service Temporary Organization shall terminate on July 4, 2026. The termination of the U.S. DOGE Service Temporary Organization shall not be interpreted to imply the termination, attenuation, or amendment of any other authority or provision of this order.

(c) DOGE Teams. In consultation with USDS, each Agency Head shall establish within their respective Agencies a DOGE Team of at least four employees, which may include Special Government Employees, hired or assigned within thirty days of the date of this Order. Agency Heads shall select the DOGE Team members in consultation with the USDS Administrator. Each DOGE Team will typically include one DOGE Team Lead, one engineer, one human resources specialist, and one attorney. Agency Heads shall ensure that DOGE Team Leads coordinate their work with USDS and advise their respective Agency Heads on implementing the President's DOGE Agenda.

Sec. 4. Modernizing Federal Technology and Software to Maximize Efficiency and Productivity. (a) The USDS Administrator shall commence a Software Modernization Initiative to improve the quality and efficiency of government-wide software, network infrastructure, and information technology (IT) systems. Among other things, the USDS Administrator shall work with Agency Heads to promote inter-operability between agency networks and systems, ensure data integrity, and facilitate responsible data collection and synchronization.

(b) Agency Heads shall take all necessary steps, in coordination with the USDS Administrator and to the maximum extent consistent with law, to ensure USDS has full and prompt access to all unclassified agency records, software systems, and IT systems. USDS shall adhere to rigorous data protection standards.

(c) This Executive Order displaces all prior executive orders and regulations, insofar as they are subject to direct presidential amendment, that might serve as a barrier to providing USDS access to agency records and systems as described above.

Sec. 5. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

THE WHITE HOUSE,

January 20, 2025.